18 May 2011

Original: English

Ninth Meeting of Heads of National Drug Law Enforcement Agencies, Europe
Vienna, 28 June-1 July 2011
Item 4 of the provisional agenda*
Implementation of the recommendations adopted by the Eighth Meeting of Heads of National Drug Law Enforcement Agencies, Europe

Implementation of the recommendations adopted by the Eighth Meeting of Heads of National Drug Law Enforcement Agencies, Europe**

I. Introduction

1. The Eighth Meeting of Heads of National Drug Law Enforcement Agencies (HONLEA), Europe, held at Vienna from 16 to 19 June 2009, adopted a set of recommendations following the consideration by working groups of the issues indicated below.

2. In accordance with established practice, the report of the Eighth Meeting was forwarded to the Governments represented at the session. A questionnaire on the implementation of the recommendations adopted at that Meeting was dispatched to Governments on 18 March 2011 together with information relating to the Ninth Meeting of HONLEA, Europe.

3. The present report was prepared on the basis of information provided to the United Nations Office on Drugs and Crime (UNODC) by Governments in reply to that questionnaire. As of 17 May 2011, replies had been received from the Governments of Croatia, Cyprus, Estonia, Germany, Israel, Luxembourg, Malta, Spain, Switzerland and Turkey.

---

* UNODC/HONEURO/9/1.

** This document has not been edited.

V.11-83105 (E)

II. Implementation of the recommendations adopted by the Eighth Meeting

Issue 1. The influence of the Internet and other electronic media on drug trafficking

Recommendation (a)

4. As a first step to ensuring an effective response to handling and recovering digital evidence, the Eighth Meeting recommended that Governments should encourage their law enforcement authorities to develop a digital evidence strategy.

5. Croatia reported that a decree on digital evidence had been passed to include in its criminal procedure act a definition of digital evidence. The act regulated the conditions under which data could be legitimately confiscated, stored and used in related cases, as well as the obligation of returning computer data (Criminal Procedure Act, articles 183, 184, 262 and 263). Subject to these provisions, recordings, documents and objects obtained by special evidentiary actions, including by intercepting, gathering and recording of computer data, could be used as evidence in court (Criminal Procedure Act, articles 332 and 333).

6. Estonia reported that Estonian police had access to all legal options for the collection and use of evidence from the media and the Internet.

7. Germany reported that the third draft of the guidelines for identification, collection and/or acquisition and preservation of digital evidence (ISO/IEC standard 27037) had been issued and that implementation of the standard was expected for the current year.

8. Israel noted that its legislation applied to crimes against computers as well as to crimes involving computer use in the perpetration of the crime (Computer Law No. 5755, 1995), and included provisions concerning evidence (Evidence Ordinance, new version, No. 5731, 1971). Specialized training courses, including modules on computer related crimes and storage of evidence, were available to police officers in order to become computer detectives.

9. Cyprus, Luxembourg, Malta and Switzerland had not taken action on this recommendation. While Malta reported that no formal national digital evidence strategy was currently applicable, such strategies had been implemented and further developed for several years by the Swiss federal and cantonal police forces.

10. Spain referred to its legislation on conservation of electronic data (law 25/2007 of 18 October 2007 on "conservation of data concerning electronic communications and public communication networks"), including the obligation for telecommunication providers to store data for use by competent law enforcement officers. Both the national police and the Civil Guard maintained special investigative units on drug trafficking via the Internet.

11. Turkey reported that the Anti-Smuggling and Organized Crime Department of the Turkish National Police had developed a fully fledged cybercrime unit and a digital evidence strategy which standardized cybercrime investigations of this department against organized crime syndicates.

Recommendation (b)

12. Because of the pressing need for a concerted worldwide response to cybercrime offences, it was recommended that Governments should be encouraged to consider the development of a United Nations convention against such offences that provides direction and guidance and supports Member States in working together to combat such offences.

13. Croatia and Germany had ratified the Council of Europe Convention on Cybercrime.[1] Malta was a signatory to the Convention and was taking steps to ratify it at the earliest opportunity.

14. Croatia reported that it had amended its Criminal Code in 2004, before it signed and ratified the Convention on Cybercrime and its Additional Protocol, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems,[2] thus introducing a number of new or modified criminal offences related to child pornography on a computer system or network, racial and other discrimination through a computer system, breach of secrecy, wholesomeness and availability of computer data, program or system, computer forgery and computer fraud.

15. Croatia and Spain also referred to the meeting of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime, Vienna, 17-21 January 2011.

16. Cyprus, Luxembourg and Switzerland had not taken action on this recommendation. Switzerland reported that its authorities had cooperated successfully on several occasions with a range of nations on cybercrime cases.

17. Germany affirmed its opposition to the adoption of a United Nations convention on cybercrime. Israel and Turkey encouraged the development of such a convention. Israel supported any international efforts in this matter and Turkey offered expert assistance in drafting such a convention.

18. Spain stated that cybercrime was a matter of priority for Member States of the European Union and referred to existing policy and legal instruments against cybercrime, including the Stockholm Programme of the European Council and the European Union Internal Security Strategy, as well as the Convention on Cybercrime and the European Union Directive on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.[3]

Recommendation (c)

19. To combat offences facilitated through the use of cybertechnologies, Governments were encouraged to ensure that their national legislation is adequate to sustain the successful investigation and prosecution of such offences within their jurisdictions.

---

[1] Council of Europe, *European Treaty Series*, No. 185.
[2] Council of Europe, *European Treaty Series*, No. 189.
[3] 2006/24/EC.

20. Croatia reported that its new criminal procedure act, which in September 2011 would replace the criminal procedure act of 1997, would shift the control and direction of criminal investigations from the judge to the state prosecutor, leaving to the judge decisions on detention, status issues of the defendant and the rights of the defendant. A new criminal code was also adopted, taking into consideration legal standards and practice of Germany, Austria and Switzerland. The code contained the obligation to proscribe international standards, including of the United Nations, the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, the European Anti-Fraud Office and the European Committee for the Prevention of Torture.

21. Cyprus, Luxembourg and Switzerland had not taken action on this recommendation. Cyprus noted that its national legislation prohibited the advertisement of narcotic substances in any way with the intent to supply it to other people. Luxembourg reported that, under its national legislation (modified law of 19 February 1973 on the resale of medical substances and the fight against drug dependence), offences related to substance abuse could be prosecuted independently from the means used to commit these offences, including through the use of cybertechnologies. Switzerland considered its current national legislation as sufficient.

22. Estonia stated that its legislation allowed the use of collected information as evidence if it was necessary to solve crimes. Germany noted that, as a party to the Convention on Cybercrime, it had adopted relevant national legislation. Israel stated that while its legislation (Computer Law, 1995) covered cybertechnology related offences, it was not always sufficient in cases where technology was more advanced, including cases related to the Internet and communications.

23. Malta reported that its legislation on computer-based crime (Computer Misuse, Chapter 9 of the Laws of Malta) was continuously updated to address emerging threats and risk assessments. As its current legislation did not contain reference to specific technologies, there was no need to re-legislate when new terminologies appeared on the market. Its law enforcement authorities were in continuous contact with various sectors, including the business communities, electronic service providers and authorities, to address emerging threats.

24. Spain reported that legislation on conservation of electronic data stipulated that such data had to be stored in order to identify the type, time, duration, origin and destiny of electronic communications, the medium used and its location, as well as the identity of users of the communication service.

25. Turkey referred to its national legislation on cybercrime (article 134 of the Turkish Law on Criminal Procedures) and reported that it was implemented through a comprehensive decree issued by the Director of the Anti-Smuggling and Organized Crime Department of the Turkish National Police.

Recommendation (d)

26. The Eighth Meeting recommended that Governments should be encouraged to establish digital evidence standards to maintain the integrity and quality of evidence gathered from cybertechnology sources.

27. Croatia reported on relevant standards in force since 2009, which proscribed technical conditions to be met by the system for audio-video recording and reproducing recordings of defendant or witness questioning, evidentiary or other actions, including evidence gathered by interception, gathering and recording of computer data, as well as minutes and handling recordings.

28. Cyprus, Luxembourg, Malta and Switzerland had not taken action on this recommendation. Malta reported that, despite the absence of a formal national strategy, its law enforcement authorities had adapted most of the "Good Practice Guide for Computer-Based Electronic Evidence" issued by the Association of the Chief Police Officers (United Kingdom of Great Britain and Northern Ireland). Annual training courses were provided to law enforcement authorities to ensure that officers entrusted with electronic investigations were conversant with the latest technical developments and measures necessary to safeguard digital evidence. Switzerland deemed additional measures not necessary, as court practice and ruling defined relevant standards of quality.

29. Estonia noted that the preservation of evidence was regulated by its code of criminal procedure.

30. Germany referred to the draft ISO/IEC standard 27037 and encouraged other countries to endorse relevant ISO norms.

31. Israel reported that when computer detectives testified in court, their testimonies were accepted together with evidence collected from various sources, such as the suspect's computer or private or public companies.

32. Spain reported that, under its legislation on conservation of electronic data, such data may only be transferred electronically to competent law enforcement officers for purposes foreseen by law and upon judicial authorization. Such data could be stored for 12 months, with the possibility of reducing or extending this period to 6 or up to 24 months in consultation with the telecommunication operator.

33. Turkey reported that the Anti-Smuggling and Organized Crime Department of the Turkish National Police had established a digital evidence strategy which functioned as a blueprint for its investigations.

Issue 2: Information: the key to dismantling trafficking groups

Recommendation (a)

34. To support a concerted and effective response by law enforcement authorities against international trafficking networks and organized crime groups, it was recommended that Governments should ensure that their national authorities make full use of the secure communication platforms, databases and other information resources available to them through participation in the Central Asian Regional Information and Coordination Centre (CARICC), the European Police Office (Europol), the International Criminal Police Organization (INTERPOL), the World Customs Organization and other trusted organizations established to support coordination.

35. Croatia reported on domestic legislation in the area of customs providing for the possibility of submitting customs declarations electronically and on its membership of relevant international bodies in this area. Its best practices in

exchanging communications electronically included the use of the Customs Enforcement Network of the World Customs Organization (WCO-CEN) and systems used by INTERPOL, as well as the agreement with Europol reached in 2010, enabling the establishment of a secure communication line between national contact points and the Europol headquarters. Croatia also referred to its activities within the Committee for Joint Cooperation of the Southeast European Cooperative Initiative (SECI) Center and its working group on preventing commercial fraud.

36. Cyprus seconded police officers both to Europol and INTERPOL, but did not participate in CARICC. Estonia maintained three police liaison officers at Europol, in order to exchange information on relevant international issues.

37. Germany referred to its longstanding support and exchange of information within the secure communication platforms, databases and other relevant information resources, including of Europol and INTERPOL.

38. The Israel Tax Authority was part of the CEN and the network of Regional Intelligence Liaison Offices (RILO) of the World Customs Organization for Western Europe.

39. Luxembourg stated that its police participated in information exchange and regular concerted operations and investigations with INTERPOL and Europol. Malta reported that it used the communication platforms mentioned in the recommendation, to exchange intelligence as well as to facilitate coordination of ongoing live investigations.

40. Spanish law enforcement officers had access to databases of INTERPOL, Europol and SIRENE through a central national office channelling all requests to these institutions. Spain had a number of liaison officers at the headquarters of both organizations and made use of the European Union liaison platforms for information exchange established in Dakar and Accra.

41. Switzerland reported that its participation in different operations, working groups and conferences of Europol, INTERPOL and others had been extended.

42. Turkey noted that, while its law enforcement agencies had access to the INTERPOL database, no access was granted to the Europol database, as Turkey was not a member of the European Union. Information exchange had been carried out via WCO-CEN, Balkan Route Data Collection and Dissemination System (coordinated by German Customs Criminal Service), and SECI. At the bilateral level, Turkish national authorities maintained channels of communication with their foreign counterparts.

Recommendation (b)

43. It was further recommended that Governments should take steps to ensure that they have established the necessary legal framework to facilitate the mutually agreed operation of foreign undercover law enforcement officers in their jurisdictions.

44. Croatia referred to its obligations under the international drug control treaties and its legislative and administrative provisions specifying the rights and obligations of joint operations with foreign undercover investigators. By the end of 2010, Croatia had signed 33 bilateral international agreements on joint law

enforcement activities. Croatian law enforcement authorities engaged in operative cooperation with their foreign counterparts both on the territory of Croatia and abroad, mainly in the field of drug control.

45. Cyprus, Israel and Turkey reported that they had not taken action to implement this recommendation. Cyprus referred to its obligation to cooperate with the Member States of the European Union pursuant to the European Union Treaty for mutual assistance in criminal matters. Israel and Turkey had no legal framework on the operation of foreign undercover law enforcement officers in their jurisdictions. Israel stated that its law enforcement agencies assessed each case individually and took appropriate measures.

46. Estonia, Germany, Luxembourg, Malta and Switzerland reported that they had established the necessary legal framework. Operations by foreign undercover law enforcement officers in Estonia were regulated by its code of criminal procedure. In Luxembourg, relevant legislation (law of 3 December 2009, law of 21 March 2006), allowed such operations also for joint investigative teams. In Malta, this was legally possible as from the year 2003, under the terms of article 435E of the Criminal Code, Chapter 9 of the Laws of Malta.

47. Spain referred to the international and national legal framework applicable to operations of foreign undercover law enforcement officers within its jurisdiction (Convention Implementing the Schengen Agreement, organic law 19/94, law 11/2003 and organic law 3/2003). An interpretation of "judicial police" was applied so as to allow such operations, which required the aim of tackling an organized crime as foreseen by law and an express authorization by the Spanish judicial authorities. The Spanish police control and supervise the foreign law enforcement officers, who would be fully subject to its national legislation while in Spanish territory.

Recommendation (c)

48. To enhance, strengthen and maintain close cooperation between law enforcement authorities engaged in the investigation of criminal networks trafficking illicit drugs, it was recommended that Governments should encourage their authorities to respond in a timely manner to requests for information and assistance from foreign counterparts.

49. Croatia referred to its international obligations and national legislation on mutual legal assistance and reported that its law enforcement authorities exchanged information with competent foreign authorities, either directly or via the Bureau of INTERPOL, Europol or the EGMONT Group of Financial Intelligence Units, and that there had been a number of cases of mutual assistance in combating international drug crime. Information exchange was also achieved through police liaison officers, present in Austria, Serbia, Israel, and at the INTERPOL (and previously Europol) headquarters, as well as at the Camden Asset Recovery Inter-Agency Network (CARIN).

50. Cyprus reported that its drug law enforcement unit cooperated and responded to all requests in a timely manner. Estonia exchanged information via its liaison officers at Europol and maintained a Sirene Bureau, from where relevant information could be obtained.

51. Germany noted that a timely response by its law enforcement authorities to requests for information and assistance was guaranteed in the majority of cases. Israel reported that agreements between Israel and its counterparts ensured timely exchange of information and assistance, including controlled deliveries. Luxembourg continued to receive such requests mainly from its neighbouring countries and exchanged information via the channels provided by INTERPOL, Europol and the Center for Police and Customs Cooperation. Malta stated that such requests were given priority and full assistance in line with Maltese Legislation and international conventions.

52. In Spain, there were police liaison offices from other States which acted as a channel for direct information exchange. Switzerland reported that additional liaison officers had been placed in key countries and that no complaints regarding timespans for its response to requests for international assistance had been received.

53. Turkey noted that its police had responded to over 1,400 information requests of its foreign counterparts in 2010 and would continue to respond information requests in a timely manner. Turkish gendarmerie and customs authorities also participated in joint operations and were involved in exchange of information with their counterparts.

Issue 3: Drug trafficking in Europe: trends, strategies and effective responses

Recommendation (a)

54. In response to the current threat posed to the States of both West Africa and Europe by transatlantic cocaine trafficking by well-organized and well-resourced criminal syndicates, the Eighth Meeting recommended that Governments should encourage their authorities to contribute to and support the Maritime Analysis and Operations Centre-Narcotics (MAOC-N) operational initiative.

55. Croatia reported that its police maintained contact and engaged in operative cooperation with the anti-narcotics initiatives MAOC-N in Portugal and CeCLAD-M in Tulone, including by involving both centres in joint operative actions with foreign authorities actions against international cocaine smuggling by sea in the Mediterranean.

56. Cyprus, Estonia, Luxembourg and Switzerland had not taken action on this recommendation. Cyprus noted that, due to its geographical position, no form of cooperation with MAOC-N existed.

57. While Germany had observer status in the MAOC-N operational initiative, Spain was one of its founding members.

58. Israel did not participate in the MAOC-N initiative but looked forward to doing so in the future. Turkey was ready to support MAOC-N, since the agency was highly concerned with transatlantic cocaine trafficking. Malta reported that while MAOC-N had not directly requested any assistance from Malta, MAOC-N and CECLAD had been involved in a controlled delivery of cocaine, carried out in collaboration with other Member States.

Recommendation (b)

59. It was further recommended that, owing to the growing use of non-commercial aircraft to traffic drugs using routes from Latin America to West Africa and from North Africa to landing points in Europe, Governments must take immediate steps to strengthen cooperation between law enforcement authorities and the general aviation sector and to support authorities in gathering the information necessary and implementing the procedures required, in order to enable those authorities to respond more effectively to the growing trafficking threat.

60. Croatia noted that the legal framework for cooperation between its prosecutorial authorities and the private sector, especially civil aviation, was in place and that its law enforcement authorities were fully cooperating on a daily basis. With reference to an example of successful cooperation with other European law enforcement authorities in a case of cocaine smuggled with small private planes from the Caribbean islands to Europe, Croatia reported that activities were underway to operationalize its internal regulation on cooperation between the Ministry of Interior and the customs administration, including action to counter international smuggling of drugs by air.

61. While Estonia had not taken action on this recommendation, Cyprus stated that close cooperation with the general aviation sector existed. Malta also reported that its law enforcement authorities had established excellent contacts with the aviation authorities in the country.

62. Germany referred to the Airport Communication Project (AIRCOP), developed by UNODC and financed by the European Union and Canada, as an example for enhancing cooperation between law enforcement authorities and the general aviation sector. Aimed at improving the capacity for international cooperation of law enforcement and judicial services, the project would focus on strengthening the anti-drug capacities of beneficiary countries at selected airports in West Africa and, in a second phase, in Latin America and Caribbean, in order to strengthen existing capacities. The project would aim at creating links and building synergies between the measures implemented in both regions.

63. In Israel, non-commercial aircrafts coming from Africa were randomly checked in collaboration with the civil aviation authority, in particular in cases of suspicion regarding their routes or other matters. Flights originating in South America were checked more often.

64. Luxembourg reported on the implementation of a system making flight information on general and sport aviation available to its police and customs authorities in real time. Its law enforcement authorities cooperated with the civil aviation sector. Reference was also made to international information exchange procedures and cooperation mechanisms, including the activities on airports of the Co-operation Group to Combat Drug Abuse and Illicit Trafficking in Drugs (Pompidou Group), mutual assistance or the directories of drug control officials at European airports and national contact officers in general aviation.

65. Spain reported on several measures adopted in the area of aviation. An agreement of 2003 between its air force and police on control of light and sport aircraft established operational procedures on communication exchange in order to control aircraft detected by the air force, which entered the national territory

without permission or in case an illicit activity was suspected, including drug trafficking. An agreement of 2006 between its Ministry of Defence and its Ministry of Interior on the fight against illicit drug trafficking included, among other measures, increased alert of the air force and the security forces on any suspicious flight. Reference was also made to the European Council conclusions on "drug trafficking — threat assessment of airfields and light aircraft" of 2010.

66. Switzerland reported that, while its customs and police carried out several control operations targeting small aircrafts and airstrips, smuggling by small aircrafts did not seem to be a major gateway for drugs into Switzerland.

67. As a target country for cocaine trafficking, Turkey attached great importance to sharing information in this field and reported that the Turkish customs administration shared information about drug seizures of European countries via the Pompidou Group, in addition to the WCO-CEN and SECI mechanisms.

III. Conclusions

68. Most Governments that returned the questionnaire had taken measures to implement the recommendations on the influence of the Internet and other electronic media on drug trafficking, or considered that their national legislation or practices already sufficiently addressed the respective recommendations. Divergent views were expressed as to whether a United Nations convention against cybercrime offences should be developed.

69. All responding Governments had taken measures to implement the recommendations on information as the key to dismantling trafficking groups, with one exception: the establishment of a legal framework for mutually agreed operations of foreign undercover law enforcement officers in their jurisdictions remained a challenge for Member States that were not bound by relevant provisions of European Union law in this area.

70. Responses by Governments diverged as to the implementation of the recommendations on drug trafficking trends in Europe. Of the significant number of Governments that did not cooperate with the MAOC-N operational initiative, some expressed their interest in supporting the initiative, while other Governments did not take action in this regard. Most Governments reported on forms of cooperation between their law enforcement authorities in the area of aviation or elaborated on the cooperation between those authorities and the general aviation sector.

71. The overview of implementation presented in the present report remains partial, as only 10 Governments out of the 56 members of the Meeting had returned the questionnaires to the Secretariat. Given that sufficient information is needed, in order to enable the Meeting to more efficiently evaluate the implementation of its recommendations, it is important that Governments complete and return the questionnaires in a timely manner.